นโยบายการกำหนดชั้นข้อมูลอันเป็นความลับ

ของ

บริษัท เด็มโก้ จำกัด (มหาชน)

นโยบายการกำหนดชั้นข้อมูลอันเป็นความลับ

1.วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้น เพื่อใช้เป็นเกณฑ์พิจารณากำหนดชั้นความลับสำหรับทุกชุดข้อมูล เพื่อลดการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดชั้นความลับของข้อมูล การรักษาความปลอดภัยของข้อมูล รวมถึงการเข้าถึงข้อมูลตามระดับชั้นความลับ โดยให้มีระบบบริหารจัดการคุ้มครองข้อมูลที่เหมาะสม มีการกำหนดมาตรการและหน้าที่ความรับผิดชอบที่จำเป็นในการรักษาความปลอดภัยของข้อมูล เพื่อบริหารจัดการให้สอดคล้องตามกฎหมาย

2. คำนิยามที่เกี่ยวข้อง

“เด็มโก้”	หมายถึง บริษัท เด็มโก้ จำกัด (มหาชน)
“การกำหนดชั้นความลับของข้อมูล”	หมายถึง การจำแนกชั้นของข้อมูลในบริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบต่อบุคคล และองค์กร หากมีการเปิดเผย เปลี่ยนแปลง หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต โดยการจัดชั้นความลับของข้อมูลช่วยกำหนดการควบคุมความปลอดภัยพื้นฐานที่เหมาะสมสำหรับการปกป้องข้อมูลนั้น ๆ
“ข้อมูลอ่อนไหว”	หมายถึง ข้อมูลอ่อนไหวเป็นข้อมูลที่มีชั้นความลับและเป็นข้อมูลที่ต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อคุ้มครองความเป็นส่วนตัวหรือความปลอดภัยของบุคคลหรือองค์กร และให้หมายรวมถึงข้อมูลส่วนบุคคลชนิดพิเศษ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย
“ข้อมูลส่วนบุคคล”	หมายถึง ข้อมูลที่เกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวตนของบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล อีเมล ที่อยู่ เบอร์โทรศัพท์ ที่อยู่จดหมายอิเล็กทรอนิกส์ที่ระบุตัวบุคคลธรรมดา IP Address รูปภาพบุคคล ซึ่งเกี่ยวข้องกับการดำเนินการต่าง ๆ ของกลุ่มธุรกิจเด็มโก้ เช่น ข้อมูลที่เกี่ยวข้องกับการจัดซื้อ จัดจ้าง และบริการอื่น ๆ เป็นต้น
“ข้อมูลอันเป็นความลับ”	หมายถึง ข้อมูลข่าวสารลับที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของบริษัท ซึ่งมีการกำหนดให้มีชั้นความลับ ตามแนวปฏิบัติฉบับนี้โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของบริษัทและประโยชน์ของบริษัทประกอบกัน

“ข้อมูลลับ”	หมายถึง ข้อมูลที่ยังมิได้มีการเปิดเผยต่อสาธารณชนหรือผ่านระบบของตลาดหลักทรัพย์เป็นการทั่วไป ซึ่งเป็นสาระสำคัญต่อการเปลี่ยนแปลงของราคาหรือมูลค่าของหลักทรัพย์ และการตัดสินใจซื้อขายหลักทรัพย์ ตัวอย่างของข้อมูลภายใน ได้แก่ 1) ฐานะทางการเงินและผลประกอบการทางการเงิน 2) การจ่ายหรือไม่จ่ายเงินปันผล 3) การเปลี่ยนแปลงมูลค่าที่ตราไว้ของหลักทรัพย์ 4) แผนธุรกิจและแผนการระดมทุน การเพิ่ม/ลดทุนโดยใช้เครื่องมือทางการเงินต่าง ๆ 5) การเปลี่ยนแปลงที่สำคัญในแผนการลงทุน หรือโครงการลงทุน 6) การร่วมทุน การควบรวมกิจการ หรือการขายกิจการ 7) การซื้อขายหลักทรัพย์ที่สำคัญ และการไถ่ถอนหลักทรัพย์ 8) การได้มา หรือสูญเสียสัญญาทางการค้าที่สำคัญของกลุ่มธุรกิจ ด็มโก้ 9) ข้อพิพาททางกฎหมายที่สำคัญ 10) การเปลี่ยนแปลงวัตถุประสงค์ของบริษัท 11) การเปลี่ยนแปลงนโยบายการบัญชีที่สำคัญ 12) การเปลี่ยนแปลงอำนาจควบคุม หรือการเปลี่ยนแปลงที่สำคัญในคณะกรรมการบริษัท หรือผู้บริหารระดับสูง
“ข้อมูล”	หมายถึง ข้อมูล ข้อความ สารสนเทศ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย
“ข้อมูลสารสนเทศ”	หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความหรือกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้ รวมถึงข้อมูลส่วนบุคคล
“ความลับทางการค้า”	หมายถึง ข้อมูลการค้าซึ่งยังไม่รู้จักกันโดยทั่วไป หรือยังเข้าถึงไม่ได้ในหมู่บุคคลซึ่งโดยปกติแล้วต้องเกี่ยวข้องกับข้อมูลดังกล่าว โดยเป็นข้อมูลที่มีประโยชน์ในเชิงพาณิชย์เนื่องจากการเป็นความลับ และเป็นข้อมูลที่ผู้ควบคุมความลับทางการค้าได้ใช้มาตรการที่เหมาะสมเพื่อรักษาไว้เป็นความลับ

“ข้อมูลการค้า”	หมายถึง สิ่งที่สื่อความหมายให้รู้ข้อความ เรื่องราวข้อเท็จจริง หรือสิ่งใดไม่ว่าการสื่อความหมายนั้นและผ่านวิธีการใด ๆ และไม่ว่าจะจัดไว้ในรูปใด ๆ และให้หมายความรวมถึงสูตร รูปแบบ งานที่ได้รวบรวมหรือประกอบขึ้น โปรแกรม วิธีการ เทคนิค หรือกรรมวิธีด้วย (พรบ.ความลับทางการค้า พ.ศ.2545)
“การเปิดเผยข้อมูลความลับ”	หมายถึง การเผยแพร่ การขาย การให้เช่าซื้อ การแจกจ่าย การทำซ้ำ การดัดแปลง และการให้เช่าต้นฉบับหรือสำเนางาน ที่เกี่ยวข้องกับ “ข้อมูลอันเป็นความลับ” ไม่ว่าทั้งหมดหรือบางส่วน ไม่ว่าจะอยู่ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ให้ข้อมูลหรือไม่ก็ตาม
“การปรับชั้นความลับ”	หมายถึง การลดหรือเพิ่มชั้นความลับของข้อมูลข่าวสารลับ และให้หมายความรวมถึงการยกเลิกชั้นความลับของข้อมูลข่าวสารลับนั้นด้วย

3. หลักการกำหนดชั้นความลับของข้อมูล

3.1. เด็มโก้ใช้ความระมัดระวังในการจำแนกชั้นความลับ ความสอดคล้องกับความอ่อนไหว และความสำคัญของข้อมูล ในการจำกัดการเข้าถึงข้อมูลจะพิจารณาในกรณีที่เป็นการเปิดเผยข้อมูลที่อาจส่งผลกระทบต่อกฎหมาย ชื่อเสียง และผลประโยชน์ของบริษัท

3.2. การกำหนดชั้นความลับของข้อมูล จะพิจารณาตามเนื้อหาและความเสี่ยงที่ส่งผลกระทบทางกฎหมาย ชื่อเสียง และผลประโยชน์ของบริษัท หรืออื่น ๆ ที่เกี่ยวข้อง โดยไม่คำนึงถึงรูปแบบ หรือแหล่งที่มาของข้อมูลที่มีจัดเก็บไว้ในระบบฐานข้อมูลของเด็มโก้ ไม่ว่าเป็นการจัดเก็บในรูปแบบ Hard Copy หรือ Electronic file ก็ตาม

3.3. เด็มโก้ จัดให้มีแนวทางการบริหารความเสี่ยงของข้อมูลที่ควรได้รับความคุ้มครองตามระดับความอ่อนไหว และความสำคัญของข้อมูล เพื่อกำหนดขอบเขตของมาตรการในการลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ อาทิ ความรุนแรง และความเป็นไปได้ที่ข้อมูลจะถูกรุกล้ำหรือถูกทำลาย หรือระดับความเสียหายที่อาจเกิดขึ้น เป็นต้น

3.4. การกำหนดระดับชั้นของข้อมูลต้องมีความเหมาะสม เพื่อให้ผู้เกี่ยวข้องได้ใช้ประโยชน์จากข้อมูลให้ได้มากที่สุด โดยมีตั้งแต่ระดับต่ำที่สุด ไปจนถึงระดับข้อมูลที่สำคัญสูง ซึ่งระดับที่สำคัญสูงจะต้องได้รับการปกป้องเพื่อรักษาความปลอดภัยของข้อมูล

3.5. ในการบริหารจัดการระบบควบคุมภายในให้เป็นไปอย่างเหมาะสม เด็มโก้ได้กำหนดบทบาทหน้าที่ของผู้มีส่วนเกี่ยวข้องกับข้อมูลที่ชัดเจน ตลอดจนสร้างความตระหนักรู้ในการบริหารจัดการและมุ่งมั่นในการรักษาความปลอดภัยของข้อมูล

4. ประเภทของชั้นความลับ

1) **ชั้นเปิดเผย (Open/Public)** หมายถึง ข้อมูลที่สามารถเปิดเผย หรือเผยแพร่ทั่วไปได้ทั้งภายใน-ภายนอก โดยไม่จำกัดการเข้าถึง
2) **ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)** หมายถึง ข้อมูลที่จำกัดการเข้าถึง หรือต้องได้รับการอนุญาตจากเจ้าของข้อมูลก่อน มีการเข้ารหัสและแยกอีเมลรหัสกับอีเมลข้อมูล หรือข้อมูลที่ไม่ได้เผยแพร่โดยอิสระ การเปิดเผยจะกระทำได้ต่อเมื่อได้รับการอนุญาตจากผู้มีอำนาจเท่านั้น และการกระทำนั้นต้องไม่ส่งผลกระทบต่อบริษัท
3) **ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ** หมายถึง ข้อมูลลับที่มีระดับสูงสุด ซึ่งหากเปิดเผยอาจก่อให้เกิดความเสียหายต่อบริษัทได้ ต้องมีการจำกัดการเข้าถึงอย่างเข้มงวด ต้องได้รับอนุญาตจากเจ้าของข้อมูล มีการเข้ารหัสและแยกอีเมลรหัสกับอีเมลข้อมูล และมีแผนปฏิบัติการฉุกเฉิน รองรับความเสี่ยง เพื่อความปลอดภัยของข้อมูล ซึ่งรวมถึงข้อมูลอ่อนไหว ข้อมูลส่วนบุคคลชนิดพิเศษตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

5. การปกป้องข้อมูลองค์กรมิให้รั่วไหลโดยแบ่งชั้นข้อมูล (DATA CLASSIFICATION)

	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
คำอธิบาย	ข้อมูลที่ได้รับความคุ้มครองตามกฎหมาย และข้อมูลที่ต้องกำหนดสิทธิ์ในการเข้าถึง หรือข้อมูลที่ถูกจำกัด	ข้อมูลที่ผู้จัดการหน่วยงานไม่มีอำนาจตัดสินใจให้เผยแพร่หรือเปิดเผยต่อสาธารณะ หรือข้อมูลที่ได้รับการคุ้มครองตามข้อผูกพันตามสัญญา หรือข้อมูลที่เผยแพร่ภายในองค์กรเท่านั้น	ข้อมูลที่ไม่มีความเป็นส่วนตัว หรือเป็นความลับ
ข้อบังคับทางกฎหมาย	มีกฎหมายกำหนดให้ต้องมีการคุ้มครองข้อมูล	การคุ้มครองข้อมูลในระดับชั้นนี้ ขึ้นอยู่กับดุลยพินิจของผู้จัดการหรือผู้ดูแลข้อมูล	
ความเสี่ยงที่ส่งผลกระทบต่อชื่อเสียง / ผลประโยชน์ของบริษัท	**มีความเสี่ยงสูง (High)**	**ปานกลาง (Medium)**	**ต่ำ (Low)**
การควบคุมการเข้าถึงระบบสารสนเทศ	ข้อจำกัดด้านกฎหมาย จริยธรรม หรืออื่น ๆ ทำให้ไม่สามารถเข้าถึงข้อมูลได้โดยไม่ได้รับอนุญาตเป็นการเฉพาะ หรือข้อมูลที่สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุมัติการเข้าถึงและลงนามในข้อตกลงว่าจะไม่เปิดเผยข้อมูล	การเข้าถึงได้เฉพาะพนักงานที่มีหน้าที่เกี่ยวข้องเท่านั้น	ไม่มีจำกัดการเข้าถึงข้อมูลสามารถเข้าถึงได้โดยอิสระ

	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
กลไกการรับ-ส่งข้อมูล	ห้ามมิให้ส่งข้อมูลที่เป็นความลับในระดับนี้ ผ่านเครือข่ายหลักที่ไม่ใช่ของของบริษัท และ/หรือห้ามส่งผ่านระบบอิเล็กทรอนิกส์ใด ๆ (เช่น อีเมลที่ไม่ใช่ของบริษัท การส่งข้อความโต้ตอบแบบทันที การส่งข้อความตัวอักษร (Line))	ไม่แนะนำให้มีการส่งข้อมูลที่ถูกจำกัดผ่านเครือข่ายไร้สายใด ๆหรือเครือข่ายแบบใช้สาย (LAN) ที่ไม่ใช่ของบริษัท หากมีความจำเป็นให้ใช้ VPN ของบริษัทเท่านั้น และ/หรือห้ามส่งผ่านระบบอิเล็กทรอนิกส์ใด ๆ (เช่น อีเมลที่ไม่ใช่ของบริษัท การส่งข้อความโต้ตอบแบบทันที การส่งข้อความตัวอักษร (Line)) ก็ไม่ควรทำเช่นกัน	ไม่จำเป็นต้องมีการป้องกันสำหรับข้อมูลเปิดเผย/สาธารณะ อย่างไรก็ตาม ควรระมัดระวังในการใช้ข้อมูลทั้งหมดของบริษัท ให้เป็นไปอย่างเหมาะสม
การจัดเก็บข้อมูล	- ห้ามจัดเก็บข้อมูลที่เป็นความลับในระดับชั้นนี้ไว้ในเครื่อง/อุปกรณ์คอมพิวเตอร์ที่ไม่ได้รับการอนุญาตจากบริษัท - ต้องมีการเข้ารหัสที่ได้รับการอนุมัติบนอุปกรณ์คอมพิวเตอร์พกพา - มีระบบรักษาความปลอดภัยในการจัดเก็บข้อมูลโดยเฉพาะการรับ – ส่ง ทางอีเมล ทั้งภายใน – ภายนอก ต้องได้รับอนุญาตจากเจ้าของข้อมูล มีเข้ารหัสและแยกอีเมลรหัส กับอีเมลข้อมูล	- ให้ปฏิบัติตามแนวปฏิบัติเรื่องการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control) กล่าวคือ มีการกำหนดสิทธิเข้าถึงข้อมูล ซึ่งจะต้องได้รับการพิจารณาอนุญาตจากผู้มีอำนาจหรือเจ้าของข้อมูล หรือผู้ดูแลระบบที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร - มีระบบรักษาความปลอดภัยในการจัดเก็บข้อมูล - ข้อมูลที่ยังไม่เปิดเผยต่อสาธารณะต้องปฏิบัติตามขั้นตอนการรักษาความปลอดภัยโดยเคร่งครัด	ไม่จำเป็นต้องมีการป้องกันใด ๆ สำหรับข้อมูลสาธารณะ อย่างไรก็ตาม ควรระมัดระวังในการใช้ข้อมูลทั้งหมดของบริษัท ให้เป็นไปอย่างเหมาะสม

	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
การสำรอง และการกู้คืนเอกสาร	จำเป็นต้องมีขั้นตอนการปฏิบัติงานในการสำรองและการกู้คืนเอกสาร	ไม่จำเป็นต้องมีขั้นตอนการปฏิบัติงานในการสำรองและการกู้คืนเอกสาร แต่ควรระบุวิธีการจัดเก็บเอกสารอย่างเป็นระบบ	
การเก็บรักษาข้อมูลที่เป็นเอกสาร	จำเป็นต้องมีแนวปฏิบัติในการเก็บรักษาข้อมูลที่เป็นเอกสาร		ไม่จำเป็นจำเป็นต้องมีแนวปฏิบัติในการเก็บรักษาข้อมูลที่เป็นเอกสาร แต่ควรระบุวิธีการจัดเก็บเอกสารอย่างเป็นระบบ
ระบบควบคุมภายใน	ผู้จัดการ/ผู้ดูแลข้อมูลที่มีหน้าที่รับผิดชอบข้อมูลที่เป็นความลับต้องตรวจสอบและทบทวนระบบและขั้นตอนสำหรับการใช้ข้อมูลในทางที่ผิดและ/หรือการเข้าถึงโดยไม่ได้รับอนุญาต พร้อมรายงานความผิดปกติให้กับเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศเพื่อวิเคราะห์ หาแนวทางแก้ไข หรือกำหนดแนวทางปฏิบัติด้านความปลอดภัยของหน่วยงาน	ผู้จัดการ/ผู้ดูแลข้อมูล ซึ่งรับผิดชอบข้อมูลที่ถูกจำกัดจะต้องตรวจสอบและทบทวนระบบและขั้นตอนของตนเป็นระยะ ๆ สำหรับการใช้ในทางที่ผิดและ/หรือการเข้าถึงโดยไม่ได้รับอนุญาต	ไม่จำเป็นต้องมีการตรวจสอบโดยผู้ควบคุมข้อมูล

	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
ตัวอย่างข้อมูล / * ข้อมูลที่ได้รับการยกเว้น	**ข้อมูลที่ได้รับการควบคุมตามกฎหมายและข้อมูลที่จะให้การเข้าถึงข้อมูลลับหรือข้อมูลที่จำกัด** คือ ทรัพยากรข้อมูลที่สามารถเข้าถึงข้อมูลที่เป็นความลับหรือถูกจำกัด (ชื่อผู้ใช้และรหัสผ่าน) ข้อมูลที่สามารถระบุตัวบุคคลที่เข้าถึงได้ กำหนดสิทธิ์การเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น เช่น - หมายเลขประกันสังคม ใบขับขี่ บัตรประจำตัวประชาชน และหมายเลขหนังสือเดินทาง ฯ - ข้อมูลทางบัญชีการเงิน เช่น เช็ค บัญชีออมทรัพย์ หมายเลขบัตรเครดิตหรือบัตรเดบิต ฯ - ข้อมูลสุขภาพ* เช่น สถานะสุขภาพ การรักษาพยาบาล ค่ารักษาพยาบาล - ข้อมูลส่วนบุคคลเฉพาะพนักงาน และ/หรือผู้มีส่วนได้เสีย - การเรียกร้องค่าชดเชยหรือความทุพพลภาพของพนักงาน - ข้อมูลทางธุรกิจ /การเงิน เช่น ข้อมูลสินเชื่อ เป็นต้น	**ข้อมูลที่ผู้จัดการตัดสินใจว่าจะไม่เผยแพร่หรือเปิดเผยต่อสาธารณะ และข้อมูลได้รับการคุ้มครองตามข้อผูกพันตามสัญญา** คือ ทรัพยากรข้อมูลที่สามารถเข้าถึงข้อมูลที่ถูกจำกัด หรือข้อมูลที่เผยแพร่เฉพาะภายในองค์กร ต้องระบุตัวบุคคลที่เข้าถึงข้อมูลได้ โดยการกำหนดสิทธิ์ผู้ใช้/รหัสผ่าน **เช่น** - ข้อมูลส่วนตัว/พนักงาน เชื้อชาติ เผ่าพันธุ์ สัญชาติ เพศ วันที่และสถานที่เกิด รูปถ่ายติดบัตรพนักงาน - ข้อมูลรายได้และข้อมูลเงินเดือน * - ขั้นตอนการปฏิบัติงาน, เอกสารระบบบริหารคุณภาพ - ข้อมูลติดต่อที่กำหนดโดยเจ้าของข้อมูล - ข้อมูลธุรกิจ/การเงิน เช่น การทำธุรกรรมทางการเงินที่ไม่มีข้อมูลที่เป็นความลับ - ข้อมูลทางธุรกิจที่ครอบคลุมและมีข้อตกลงที่จะต้องไม่เปิดเผยข้อมูล - บันทึกการใช้จ่าย การกู้ยืม มูลค่าสุทธิ	**ข้อมูลที่ไม่คาดว่าจะมีความเป็นส่วนตัวหรือเป็นความลับ หรือข้อมูลติดต่อที่ได้รับความยินยอมจากเจ้าของข้อมูลแล้ว /ข้อมูลของบริษัทที่เปิดเผยแล้ว** - ชื่อ ที่อยู่ ที่อยู่อีเมล - หมายเลขโทรศัพท์ที่แสดงในบริษัท ปริญญาเกียรตินิยมและรางวัล สถาบันการศึกษา สาขาวิชาที่เรียน - วันที่ทำงาน ตำแหน่งปัจจุบัน ข้อมูลธุรกิจ - แผนที่บริษัท - ประกาศรับสมัครงาน - สิ่งพิมพ์/ประชาสัมพันธ์ของบริษัท

	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private)	ชั้นเปิดเผย (Open/Public)
		- งานวิจัยที่ไม่ได้ตีพิมพ์หรือรายละเอียดงานวิจัย/ผลงาน/นวัตกรรมที่ไม่ใช่ข้อมูลลับ - ข้อมูลส่วนบุคคล ที่ได้รับความยินยอมและฐานตามกฎหมาย เช่น การจ้างงาน , การประเมินผลงาน ข้อมูลครอบครัว (คู่สมรส คู่ครอง บุตรฯลฯ) ข้อมูลทางการแพทย์ - ข้อมูลผู้บริจาคที่ไม่ระบุชื่อ (และ/หรือชื่อองค์กร ถ้ามี) พร้อมข้อมูลของขวัญประเภทใดก็ได้ (เช่น จำนวนเงินและวัตถุประสงค์ของข้อผูกมัด) ข้อมูลผู้บริจาคอื่น ๆ เช่น นามสกุล ชื่อจริง หรือชื่อย่อ (และ/หรือชื่อองค์กร ถ้ามี) หมายเลขโทรศัพท์/โทรสาร อีเมล และ - ข้อมูลเกี่ยวกับการบริหารจัดการภายในองค์กร - รายละเอียดข้อมูลงบประมาณประจำปี - การเปิดเผยความขัดแย้งทางผลประโยชน์ - ข้อมูลการลงทุนของบริษัท	
หมายเหตุ : * ประเภทข้อมูลได้รับการคุ้มครองตามกฎหมาย และหรือได้รับการยกเว้นหรือได้รับความยินยอมเป็นการเฉพาะเพื่อประโยชน์สูงสุดของเจ้าของข้อมูล			

6. แนวปฏิบัติที่ดี

6.1. บุคลากร พนักงาน ที่สามารถเข้าถึงข้อมูลอันเป็นความลับ ในชั้นความลับใดก็ตาม จะต้องเป็นบุคคลที่ผู้บังคับบัญชามอบหมายความไว้วางใจ และให้เข้าถึงข้อมูลอันเป็นความลับ ได้เฉพาะเรื่องที่ได้รับมอบหมายเท่านั้น และมีหน้าที่รักษาความลับและความปลอดภัยของข้อมูล เพื่อปกป้องข้อมูลอันเป็นความลับ และเพื่อไม่ให้ข้อมูลอันเป็นความลับถูกเปิดเผย

6.2. ข้อมูลที่เป็นความลับและข้อมูลที่ถูกจำกัดต้องได้รับการเก็บรักษาอย่างปลอดภัย ถูกต้อง และเชื่อถือได้ และพร้อมสำหรับการใช้งาน โดยผู้ที่ได้รับอนุญาตมีมาตรการรักษาความปลอดภัยที่แตกต่างกันไปตามความเหมาะสมกับระดับที่ข้อมูลจะสูญหายหรือเสียหาย หรือทำให้ธุรกิจเสื่อมเสีย เสียหาย หรือละเมิดกฎหมาย นโยบาย หรือสัญญา มาตรการรักษาความปลอดภัยของข้อมูลกำหนดโดยเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ และผู้จัดการหน่วยงานที่ดูแลข้อมูล

6.3. การกำหนดมาตรการรักษาความปลอดภัยของข้อมูล ต้องมีการประเมินความเสี่ยงด้านมูลค่าของข้อมูล ความละเอียดอ่อน ชื่อเสียง หรือผลประโยชน์ของบริษัท เพื่อใช้การรักษาความปลอดภัยในระดับที่เหมาะสม

6.4. กำหนดให้ผู้จัดการหน่วยงาน มีหน้าที่รักษาดูแลข้อมูลอันเป็นความลับ โดยจัดทำตารางควบคุมรายการเอกสารข้อมูลอันเป็นความลับในหน่วยงานของตน (ตามแบบฟอร์ม) โดยจะต้องรักษาข้อมูลอันเป็นความลับให้ปลอดภัย การจำกัดบุคคลเข้าถึงข้อมูลอันเป็นความลับ หรือหากมีการเปิดเผยข้อมูลอันเป็นความลับแก่ผู้ใด ต้องกระทำโดยระมัดระวัง พร้อมจัดทำแผนปฏิบัติการฉุกเฉินกรณีที่ข้อมูลอันเป็นความลับที่มีความเสี่ยงสูง เกิดการรั่วไหล หรือถูกโจรกรรมข้อมูล หรือข้อมูลสูญหายให้สอดคล้องตามนโยบายของบริษัท

6.5. จัดให้มีการตรวจสอบข้อมูลที่ได้รับการจัดชั้นความลับ เพื่อให้แน่ใจว่าข้อมูลอันเป็นความลับได้ถูกจัดเก็บอย่างเหมาะสม ปลอดภัย และมีแผนรองรับความเสี่ยงของข้อมูลความลับที่มีความเสี่ยงสูงนั้น ๆ หากพบว่ามีการจัดการข้อมูลไม่ถูกต้องหรือไม่เหมาะสม ให้แจ้งผู้เกี่ยวข้องรีบดำเนินการแก้ไขทันที

6.6. กำหนดให้เจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ มีหน้าที่กำหนดสิทธิ์การเข้าถึงและการนำข้อมูลไปใช้อย่างเหมาะสม โดยได้รับการอนุมัติจากผู้จัดการหน่วยงานก่อนที่จะให้สิทธิ์ในการเข้าถึง และทบทวนสิทธิ์การเข้าถึงอย่างน้อยปีละ 1 ครั้ง รวมถึงรับผิดชอบทางเทคนิคขั้นสูงสำหรับการปกป้องคุ้มครองข้อมูล เพื่อให้การดำเนินงานด้านเทคโนโลยีมีประสิทธิภาพ

6.7. หากพบว่าข้อมูลสูญหาย ถูกลบหรือถูกละเมิดข้อมูล ให้ผู้ทราบข้อเท็จจริงรายงานข้อเท็จจริงที่เกี่ยวข้องให้ผู้จัดการทราบ เพื่อพิจารณารายงานการละเมิด

- กรณีข้อมูลที่จัดอยู่ในรูปแบบ Electronic file และอยู่ในระบบคลาว์ของบริษัท ให้แจ้งไปยังเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศดำเนินการตรวจสอบการกระทำที่เกี่ยวกับข้อมูลที่ถูกละเมิดนั้น ประเมินผลกระทบที่เกิดขึ้นและรายงานไปยังผู้บริหารสูงสุดสายงานเทคโนโลยี

สารสนเทศ เพื่อรายงานต่อคณะกรรมการบริหาร ทั้งนี้ให้ปฏิบัติตามนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

- กรณีข้อมูลที่อยู่ในประเภท Hard Copy หากพบว่าข้อมูลสูญหาย ถูกลบหรือถูกทำลาย โดยไม่ชอบ ให้ผู้พบเห็นแจ้งเหตุไปยังหน่วยงานตรวจสอบภายใน เพื่อดำเนินการสอบสวนหาข้อเท็จจริง และรายงานผลต่อคณะกรรมการบริหาร และคณะกรรมการตรวจสอบทราบ

6.8. จัดให้มีการสื่อสารและฝึกบอรมอย่างต่อเนื่องแก่พนักงาน เพื่อให้เกิดความรู้ ความเข้าใจอย่างแท้จริงเกี่ยวกับมาตรการและความรับผิดชอบที่จำเป็นสำหรับการรักษาความปลอดภัยของข้อมูล ความคาดหวัง และบทลงโทษหากไม่ปฏิบัติตามนโยบายฉบับนี้

7. ช่องการติดต่อ

เด็มโก้ กำหนดให้หน่วยงานกำกับและควบคุม มีหน้าที่ให้คำปรึกษาและข้อแนะนำเกี่ยวกับนโยบายฉบับนี้ เพื่อให้การปฏิบัติงานสอดคล้องตามหลักการกำหนดชั้นความลับของข้อมูล และตามหลักการกำกับดูแลกิจการที่ดี

8. การติดตามผล การทบทวนและการปรับปรุง

เด็มโก้ กำหนดให้หน่วยงานตรวจสอบภายใน มีหน้าที่สอบทานความเพียงพอ เหมาะสมและประสิทธิภาพของระบบควบคุมภายใน และการปฏิบัติตามนโยบายฉบับนี้ หากพบว่ามีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องกับข้อมูลอันเป็นความลับได้รู้หรืออาจรู้ถึงข้อมูลอันเป็นความลับ หรือเมื่อสงสัยว่ามีการละเมิดการรักษาความลับของข้อมูลข่าวสารของบริษัท ให้ดำเนินการสอบสวนโดยไม่ชักช้า และรายงายผลต่อคณะกรรมการตรวจสอบทราบ

9. บทลงโทษ

หากพบว่าพนักงาน หรือผู้ที่เกี่ยวข้อง มีการละเมิด หรือไม่ปฏิบัติตามมาตรการตามนโยบายฉบับนี้ และนโยบายที่เกี่ยวข้องกับนโยบายนี้ พนักงานหรือผู้เกี่ยวข้องนั้นอาจถูกระงับหรือการยุติการเข้าถึง และอาจมีการลงโทษทางวินัย ตามระเบียบข้อบังคับ หรือตามที่กำหนดไว้ในนโยบายที่เกี่ยวข้องอื่น ๆ หรือมีโทษทางแพ่งหรือทางอาญา ตามแต่กรณี

10. นโยบายและแนวปฏิบัติที่เกี่ยวข้อง

- นโยบายการทำสัญญาปกปิดความลับ
- นโยบายการจัดการข้อมูลลับและข้อมูลที่อาจมีผลกระทบต่อราคาหลักทรัพย์
- แนวปฏิบัติเรื่องการควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)

กฎบัตรนี้ได้รับความเห็นชอบจากที่ประชุมคณะกรรมการกำกับดูแลกิจการและความยั่งยืน ครั้งที่ 5/2566วันที่ 20 ธันวาคม 2566 และได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 8/2566 วันที่ 26 ธันวาคม 2566